**South African Journal of Information Management**
ISSN: (Online) 1560-683X, (Print) 2078-1865

# Optimum systems integration architecture for monitoring to manage an electricity utility

**Authors:**
Sello S. Pokane[1]
Musa C. Shilenge[2]
Arnesh Telukdarie[2]

**Affiliations:**
[1]Postgraduate School of Engineering Management, Faculty of Engineering and Built Environment, University of Johannesburg, Johannesburg, South Africa

[2]Johannesburg Business School, University of Johannesburg, Johannesburg, South Africa

**Corresponding author:**
Arnesh Telukdarie,
arnesht@uj.ac.za

**Dates:**
Received: 16 Feb. 2022
Accepted: 19 May 2022
Published: 08 Nov. 2022

**How to cite this article:**
Pokane, S.S., Shilenge, M.C. & Telukdarie, A., 2022, 'Optimum systems integration architecture for monitoring to manage an electricity utility', *South African Journal of Information Management* 24(1), a1525. https://doi.org/10.4102/sajim.v24i1.1525

**Background:** A Supervisory Control and Data Acquisition (SCADA) system is critical for remote monitoring and control of devices in various industries such as power utilities, oil and gas refineries, and manufacturing. Previous generations of SCADA systems have numerous limitations in today's business environment. The latest technological advancements have brought forth new SCADA architecture variants that can be configured to ensure optimised operations. There is a need to assess the latest SCADA architectures that are posed to replace previous generations.

**Objectives:** This research study aims to review various SCADA architectures and proposes an optimum SCADA system architecture for power utility. The proposed architecture is compared with the existing power utility SCADA system to highlight the impact and benefits of the proposed architecture.

**Methods:** The research uses a qualitative approach and a comparative case study method to compare 10 SCADA architectures against a literature review-based criterion. A Multi-Criteria Decision-Making (MCDM) matrix is used to evaluate SCADA architectures and proposes an optimum Internet-of-Things (IoT)-SCADA system architecture for the power utility case study.

**Results:** The research proposed an IoT-SCADA system architecture for optimum system functioning and compared the proposed architecture with the existing utility SCADA architecture. Moreover, the impact and benefits of the proposed architecture to the utility company are presented.

**Conclusion:** The proposed IoT-SCADA system architecture has the potential to resolve many of the challenges encountered with previous generations of SCADA system architectures.

**Keywords:** IoT; SCADA; cybersecurity; integration; industry 4.0.

## Introduction

Organisations' and countries' economic growth and sustainability largely depend on the critical infrastructure such as power stations, oil and gas refineries. Numerous organisations use Supervisory Control and Data Acquisition (SCADA) systems to control and monitor critical infrastructures (Bobat, Gezgin & Aslan 2015). Li et al. (2017) indicated that a SCADA system provides local and remote monitoring of the processes, equipment and devices in real time. The major components of a typical power utility SCADA system consist of a human machine interface (HMI), master terminal unit (MTU), remote terminal unit (RTU), programmable logic controller (PLC), data historian server and communication infrastructure. The functional requirements of the SCADA system include data acquisition, equipment remote control, parameter measurements, and monitoring of device statuses and warning alarms. Therefore, all the major components must be appropriately integrated in terms of the SCADA system's hardware and software to fulfil the monitoring and control functions.

Furthermore, the communication infrastructure is critical for a SCADA system because it ensures that the data from field equipment reach the control centre timeously by providing a link between MTU and field RTUs. The wired and wireless communication mediums commonly used include optical fibre, copper, radio and General Packet Radio Service (GPRS). Because of the seamless and less demanding implementation process, the GPRS technology provides an immense advantage for remote monitoring (Yadav & Paul 2021). Sighania and Kinker (2015) and Kopte (2015) summarised the power utility's benefits of a properly implemented SCADA system. Examples of the advantages include quicker power restorations and savings on operational costs.

With the advent of industry 4.0 (I4.0) technologies, a SCADA system provides organisations with the advantage of implementing an intelligent grid system (Sighania & Kinker 2015). Stanimirović et al. (2020) mentioned that the benefits of SCADA systems in the 21st century mainly include plant remote monitoring and control. However, the system must support the organisational strategy and objectives.

This research study seeks to answer the following questions:

- Which SCADA system architecture is appropriate for systems integration to ensure optimum operation of the SCADA system for a power utility company?
- What is the difference between the current power utility company SCADA system and the proposed optimum SCADA system architecture?
- What are the benefits and impact of the proposed SCADA system architecture on the power utility company?

This research study is structured as follows: The following section presents a literature review by discussing crucial subjects such as the evolution of the SCADA system, enterprise systems integration, Internet-of-Things (IoT) and cybersecurity. Then follows the research methodology section that presents the research approach and methods employed to address the research questions. Next, the results section presents the SCADA systems architecture assessment outcome, followed by the discussion section that discusses the study results. Finally, the last section concludes the study and presents the limitations and related future work.

NB: This study uses industrial control systems (ICS) and SCADA systems interchangeably.

# Literature review

## Evolution of the SCADA system

Supervisory Control and Data Acquisition systems were in use before the third industrial revolution introduced silicon-chip-based automation and information technology. The SCADA system has evolved through four generations (Rajeswar 2019), discussed in the following sections.

## The Monolithic SCADA system

The monolithic SCADA system is the first-generation SCADA system that cannot connect with other systems. The system uses a wide area network (WAN) for communication between RTUs and the master station. As a result, only devices from the same vendor communicate using proprietary protocols (Subramanian 2017).

## Distributed SCADA system

The distributed SCADA system is the second generation that communicates in small networks such as the Local Area Network (LAN) (Subramanian 2017). The small networks offer a more reliable network because of sharing computational services such as operator interfaces, communication processors, database servers and historian servers. On the contrary, interoperability of heterogeneous devices is not possible in this SCADA system. Therefore, the RTUs and master station use WAN and LAN to communicate in this SCADA system architecture.

## Networked SCADA system

The networked SCADA systems primarily use networks and the web because of cost-effective solutions and changes brought forth by international standards for communication and open protocols (Yadav & Paul 2021). Data transmission between the RTUs and master station uses protocols such as Distributed Network Protocol (DNP3), Internet Protocols (IPs) and International Electro-Technical Commission (IEC) 60870-5-101/104. Additionally, the protocols support interoperability between heterogeneous devices and systems.

## Internet-of-Things-Supervisory Control and Data Acquisition (IoT-SCADA) system

The latest generation is the IoT-SCADA system, which is the SCADA version of the typical Industrial Internet-of-Things (IIoT). The fourth generation uses the latest technologies, such as the IoT, combined with the latest SCADA hardware and software. The IoT is a network of physical things that fosters interaction between people, people with machines and between machines through the internet (Patel, Patel & Scholar 2016). All the devices have a distinctive identity to connect to the internet and communicate data autonomously in the IoT-SCADA system (Flaus 2019).

Moreover, the IoT-SCADA is critical to resolving the limitations of the traditional SCADA systems architectures in the evolving business environment. The challenges of the conventional SCADA systems architectures include the inability to access sensor nodes directly (Postolache, Sazonov & Mukhopadhyay 2019), the inability to accommodate rapid changes, inflexibility and static (Shahzad, Kim & Elgamoudi 2017).

Industry 4.0 technologies include technologies such as Cyber-Physical Systems, IoT, cloud computing and smart factories (Aly, Khomh & Yacout 2021). Furthermore, technologies such as the IoT can provide a solution to the challenges of traditional SCADA systems. Hence, IoT is an essential technology for a smart substation (Hossain et al. 2019).

Cloud computing has advanced IoT technology in power distribution (Tom & Sankaranarayanan 2017). The advancements are because of fog computing's prompt data processing, fast response and faster communication networks. Fog computing provides the link between the cloud and sensing devices. The sensing devices in the power network include smart energy meters, line sensors such as voltage transformers and intelligent electronic devices (IEDs). The cloud provides data storage, demand prediction, high-level processing with historical data, utility billing systems and so on.

### IoT-SCADA system enabling technologies

Integrating SCADA systems and IoT technologies provides numerous advantages compared with previous SCADA systems. The advantages include flexibility, data analytics, interoperability and standardisation (Kaur 2018). Nonetheless, the supporting technologies must integrate the IoT-SCADA system appropriately for the organisation to realise the benefits. The supporting technologies for IoT include cloud computing, big data storage, wireless sensor networks, machine-to-machine communication and wireless communication networks (Paul & Saraswathi 2017; Rajeswar 2019). Furthermore, Pramudhita et al. (2018) and Borgaonkar and Jaatun (2019) added that the IPv6 addressing provides a solution for identifying objects in IoT architectures because IPv6 can accommodate a vast number of unique addresses.

However, the IoT-SCADA system poses significant cybersecurity risks to enterprise systems due to the connection of several devices to the public internet. Internet-of-Things network protocols such as Transport Layer Security/ Secure Socket Layer (TLS/ SSL) are critical to overcome some of the cybersecurity risks (Subramanian 2017). Yadav and Paul (2021) and Da Silver et al. (2016) provide more details on other IoT-SCADA protocols, such as Message Queuing Telemetry Transport (MQTT). Security measures such as safety pre-checks on individual system components and scanning traffic of various security protocols can bring latency to data communications (Januário et al. 2016). Hence, appropriate trade-offs between latency and security measures are essential. To resolve some of the challenges of the IoT-SCADA system, Borgaonkar and Jaatun (2019) recommended the use of 5G cellular networks because of the IoT enabling features, such as high bandwidth, ultra-high wireless speed, very low latency and flexibility.

Cloud computing is another critical enabler of the IoT-SCADA system that provides access to technical services such as data storage and processing capabilities. The National Institute of Standards and Technology (NIST) defines cloud computing as a model that supports network access to a shared number of resources with internet connection capabilities (April, Ouanouki & Morales 2014). Shared resources include networks, servers, data storage, applications and services. Cloud computing service providers allocate a virtual Information Technology (IT) framework and data centres with software and hardware to broaden and share the resources according to the customer’s requirements (Zawra, Mansour & Messiha 2019). Rani, Rani and Babu (2015) provide details on deployment models, service models, and security risks and challenges. Cloud computing deployment models include public, private, hybrid and community cloud. Nevertheless, Shahzad and O’Nils (2018) argue that the IoT-SCADA supporting technologies still require further development.

### IoT system architecture

As shown in Table 1, the physical layer involves collecting raw data from sensors and actuators, and the network layer provides communication infrastructure to link the application and physical layers. Furthermore, the internet infrastructure offers communication links. Finally, the application layer provides data storage, fast processing, analytics and management through the cloud computing servers.

**TABLE 1:** Layers, stages and components of Internet-of-Things system.

| IoT Layers | IoT Components and services |
|---|---|
| Application layer | **Cloud/data servers**<br>Storage, processing, analytics, management |
| Network layer | **Internet infrastructure\|fog servers**<br>Gateways, ISPs.\|servers for pre-processing |
| Physical layer | **Physical devices**<br>Sensors and/or actuators |

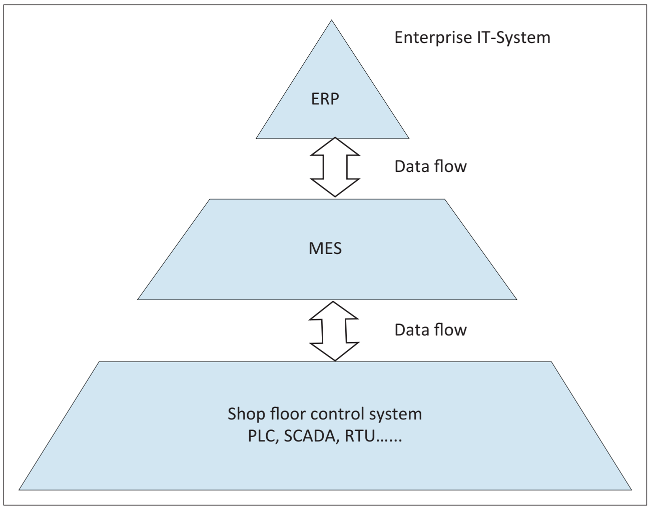
*Source*: Shahzad, K. & O’ Nils, M., 2018, *Condition monitoring in industry 4.0 -design challenges and possibilities: A case study*, pp. 101–106, IEEE, Brescia

## The enterprise systems integration architectures

### Traditional enterprise system hierarchy

The research explored the data flow across ICS and the Enterprise Resource Planning (ERP) through the Manufacturing Execution System (MES) of the traditional enterprise system hierarchy (see Figure 1). The MES forms part of the Manufacturing Enterprise Solutions Association (MESA). The MESA provides a reference model for enterprise systems integration in the manufacturing and production industry (Lundius 2019).

As shown in Figure 1, the bottom layer represents ICS components such as SCADA, RTU, PLC and the like. The MES is the central layer that collects data, processes, and distributes information from the ICS and ERP layers to optimise production activities from orders to completed products. Finally, the top layer represents enterprise management functions such as business planning and logistics, human Resources (HR), Finance and so on. Hain et al. (2017) presented an improved MES model (c-MES) to demonstrate the



*Source*: Lundius, A., 2019, *Initial assessment of manufacturing execution systems*, pp. 3–17, Royal Institute of Technology, Stockholm, viewed 20 February 2021, from https://kth.divaportal.org/smash/get/diva2:1374272/FULLTEXT01.pdf

ERP, Enterprise Resource Planning; MES, Manufacturing Execution System; PLC, programmable logic controller; SCADA, supervisory control and data acquisition; RTU, remote terminal unit.

**FIGURE 1:** Traditional enterprise system hierarchy.

integration of various enterprise systems with other support functions for improved enterprise systems operation.

## The leading systems integration architectures

Wang Towara and Anderl 2017 presented the use of the Reference Architecture Model for Industry 4.0 (RAMI4.0), Industrial Value Chain Reference Architecture (IVRA), and Industrial Internet Reference Architecture (IIRA) as the future leading architectures. The indicated architectures are vital to aid smart future factories' implementation. However, models such as the RAMI4.0 are in their infancy and have only seen implementation at research institutions or associations on a small scale (De Melo & Godoy 2019; Binder et al. 2020).

## Improved secure network architecture

The International Society of Automation 99 (ISA)-99 Committee for Manufacturing and Control System Security uses the Purdue model as a reference for ICS network segmentation (Ackerman 2017). Purdue model provides operating zones for devices and equipment into hierarchical functions for integrated enterprise systems. Furthermore, Obregon and Barbara (2015) demonstrated the improved Purdue model to secure integrated enterprise systems and ICS against cyber-attacks. The enhanced model has two Demilitarised Zones (DMZ). The first DMZ is between the ICS and ERP, and the second DMZ is between ERP and interaction with the external world, such as businesses-to-businesses (B2B) communications.

Additionally, the ISA-99 standard further provides a generic reference model for the integrated manufacturing system to indicate the functionality level of various enterprise systems (ISA 99 2007). The ISA-99 standard explains numerous security measures for the SCADA system in conjunction with functional hierarchy levels. Integrating the IT systems and SCADA system requires a detailed risk assessment because of the different security requirements of the two systems. Therefore, the risk assessment process must consider the system requirements, industrial standards and practices, and regulatory standards for integration (Obregon & Barbara 2015). The United States Industrial Control Systems – Cyber Emergency Response Team (US ICS-CERT) provides a risk management approach for ICS operation (ICS-CERT 2016).

## IT versus industrial control systems integration security and considerations

Upadhyay and Sampalli (2020) compared IT and SCADA systems security requirements and systems integration consideration as follows:

- Security mechanism – IT systems are mainly concerned with protecting data, while ICS systems are concerned with the availability of the plant. It is not easy to install, test, configure and upgrade ICS security because of the need for continuous operation of the network and required high uptime (Dolezilek, Gammel & Fernandes 2019).
- Vulnerabilities management – Many ICS systems are vulnerable to malware attacks because of legacy devices with weak architectural designs. The ICS devices require routine patch updates for security, and usually, only the original equipment manufacturer can apply the updates. While on the IT network, security updates occur automatically using a central system management software.
- Operational environment – ICS devices operate on the shop floor and in harsh environments, while IT devices operate in conducive business facilities.
- Devices/components lifespan – ICS devices typically have a longer lifespan than IT devices.

## Standard Industrial Control systems security practices

Organisations can reduce cyber-attacks and ensure secured operational systems using some of the countermeasures listed below (US ICS-CERT 2016):

- The organisation must identify, reduce and protect all network interfaces to ICS, including network endpoints that make a direct or indirect interface. The endpoint is a component or device with computational capabilities and network connectivity (Filkins & Doug 2018).
- The unused services, ports and protocols must be disabled.
- Use security features and implement solid configuration management practices.
- Perform continuous assessment and monitoring of ICS networks and interfaces.
- Adopt a risk-based defence-in-depth method.
- Proper employee management includes establishing performance expectations, establishing security policies and providing security training.

The abovementioned countermeasures are not exhaustive but highlight the minimum protection measures. Cybersecurity standards such as ISA-99 and NIST 800-82 provide more detail on the countermeasures.

## SCADA systems' contribution to power utility management

Some of the contributions of the SCADA system in the organisation management are as follows:

- The SCADA system data aid with equipment statistical reports critical to tracking maintenance Key Performance Indicators (KPIs) (Ivanković et al. 2018).
- Load monitoring and control of the electric power network ensure effective energy demand and supply management (Madala et al. 2018).

Sighania and Kinker (2015) further emphasised that the use of the SCADA system in conjunction with Geographical Information Systems (GIS) provides the following benefits to the organisation:

- Real-time fault alarming and geolocation on the power network.
- Reduced operational and maintenance costs due to a reliable power network.

- Reduction of workforce from the plant allows for the redeployment of employees to functions that lack resources, thus improving organisational performance and agility.

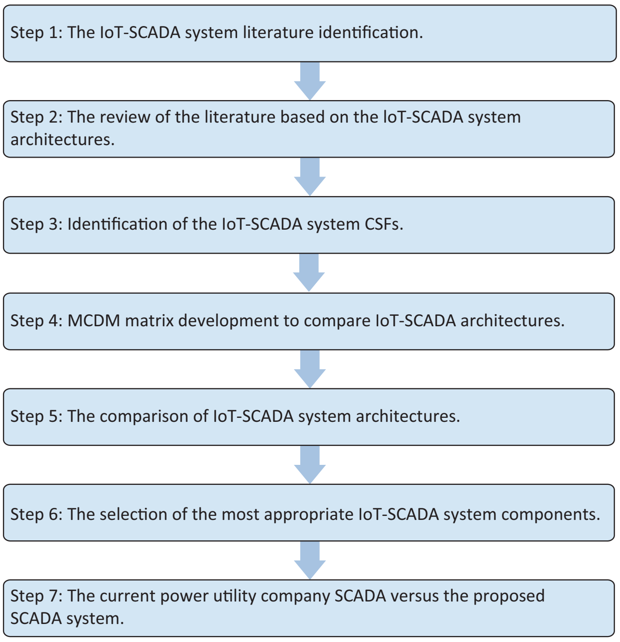
# Research methodology

## Research strategy and methods

The research uses a qualitative approach and a comparative case study method to compare 10 IoT-SCADA architectures against the criteria rooted in the literature. Figure 2 depicts a graphical representation of the research methodology steps.

The architecture comparison involves collecting and identifying the relevant IoT-SCADA literature through an online academic database search. The database search keywords are as follows: IoT, SCADA system, architectures, monitoring and integration. The period of the database search starts from the year 2015 to 2021.

A list of critical successful factors (CSFs) of an IoT-SCADA system is developed, which have a collective impact on the optimum integration of the IoT-SCADA system. A multi-criteria decision-making (MCDM) matrix is used to evaluate the identified CSFs of the IoT-SCADA architectures (Kumar et al. 2020). One of the advantages of the MCDM is that it permits decision-makers to consider all the criteria factors to reach the proper conclusion. Because of transparency and the use of basic calculations, the MCDM applies the weighted sum method (WSM) from various approaches, such as analytical hierarchy process (AHP), technique for order preference by similarity to ideal solution (TOPSIS) and fuzzy-AHP. In this study, the MCDM method uses the qualitative comparative analysis (QCA) fuzzy-set technique to assess the 10 IoT-SCADA architectures (Nigel & Vera 2017). The fuzzy-set approach sets the degree of the presence and absence of the factors using a 5-pointer scale. Furthermore, the fuzzy-set approach can provide a profound and substantial understanding of data (Hong, Xia & Guangrong 2020; Pappas et al. 2016). The criteria scores to rate CFSs are between zero and one, with 0 indicating the poor application (the lowest score), 0.25 indicating a fair application, 0.5 showing average application, 0.75 indicating good application and 1 displaying excellent application (highest score) of the concept.


Step 1: The IoT-SCADA system literature identification.
Step 2: The review of the literature based on the IoT-SCADA system architectures.
Step 3: Identification of the IoT-SCADA system CSFs.
Step 4: MCDM matrix development to compare IoT-SCADA architectures.
Step 5: The comparison of IoT-SCADA system architectures.
Step 6: The selection of the most appropriate IoT-SCADA system components.
Step 7: The current power utility company SCADA versus the proposed SCADA system.

IoT-SCADA, Internet-of-Things-Supervisory Control and Data Acquisition; CSF, critical successful factors; MCDM, Multi-Criteria Decision-Making.

**FIGURE 2:** Data collection and analysis process.

## Research case

The research case study is of a power utility SCADA system. The aim is to properly integrate the SCADA system components for the optimum operation of the power utility using academic literature and advancements in new technologies such as IoT.

# Results

## IoT-SCADA system literature search and selection

### Literature searching

The search for the literature to answer the research questions is through the online electronic resource of the IEEE, Knovel, Google Scholar, and ScienceDirect databases. The search process initially identified 50 articles using the search keywords.

### Literature classification

The classification of the articles involved sorting literature according to the years and databases. Most of the literature is from 2017, 2019 and 2020, and fewer articles are from 2015. In classifying the distribution of the identified articles per database, the IEEE and ScienceDirect database produced 58% (29 papers) and 32% (16 papers) of the literature, respectively. Knovel produced 8% (4 papers), and Google Scholar yielded 2% (1 paper).

### The selection of the relevant literature

The process of selecting the relevant studies involves the following. Firstly, manual reading of the article's title and abstract to check if the studies match the research objectives; secondly, using the selection criteria in Table 2. This process guides the addition or removal of articles from a relevant studies list. In the end, the process yielded the identification of 20 articles relevant to the IoT-SCADA system.

### Identification of the Critical Successful Factors for the IoT-SCADA system architecture

The criteria for optimum integration of the IoT-SCADA system are based on 10 relevant literature studies presented in Table 3. The 10 articles form part of the 20 identified relevant IoT-SCADA system literature. The selection of the 10 studies is as follows: firstly, the studies have clearly explained IoT-SCADA architectures. Secondly, the studies thoroughly describe the IoT-SCADA system CSFs. Internet is common in all architectures.

Table 3 summarises the identified CSFs for optimum integration of the IoT-SCADA system based on the literature review.

### Multi-Criteria Decision-Making matrix scoring

The study developed a rating criteria rubric and an MCDM matrix to evaluate the architectures. The rating criteria rubric is as per the QCA described in the research methodology.

The following equations describe the calculations of the MCDM matrix scoring presented in Table 4:

1. Category score (%) = ∑ ((Criteria rubric rating scores) × Criteria weightings (%))
2. Total architecture score (%) = ∑ (Categories weightings).

The integration of enterprise systems is a challenge, with new concepts, frameworks and models being proposed and modified in the literature as the field matures. New technologies associated with industry 4.0, such as IoT, fog and cloud computing, have numerous advantages for telemetry-based systems, such as a SCADA system for power utilities. The case study in this research seeks to contribute to the literature using new technologies as components to form an optimum IoT-SCADA system architecture for the power utility based on the review of current literature. The results of the MCDM matrix consolidate the components of the proposed IoT-SCADA system. The combination of highly scored components is accepted as proof of the criticality of the particular components to successful integration in IoT-SCADA systems. Moreover, the security implications of various architectural features were considered. The results and implications of the MCDM matrix are discussed in the next section.

**TABLE 2:** The studies selection criteria.

| Item no | Inclusion | Exclusion |
|---|---|---|
| **Articles selection criteria** | | |
| 1 | Papers published in the year 2015 to 2021 | Papers published before the year 2015 |
| 2 | Articles must be in English | Articles not written in English |
| 3 | Articles with source references | Articles without source references |
| 4 | Articles based on IoT-SCADA architectures, IoT components, and IoT-SCADA enabling technologies | Articles without the IoT-SCADA architectures, IoT components, and IoT-SCADA enabling technologies |
| 5 | Clear study objectives | Unclear study objectives |
| 6 | A clear description of the proposed architecture | Unclear definition of the proposed architecture |
| 7 | - | Repeated articles |

IoT-SCADA, Internet-of-Things-Supervisory Control and Data Acquisition.

## Discussion

In evaluating IoT-SCADA architectures, the research compared 10 architectures against the defined criteria of literature-grounded CSFs. Table 3 depicts the results of the architecture comparison using the MCDM matrix.

From the MCDM matrix results, study S3 is rated the highest with 79%, while S4 and S6 are rated the lowest, with 43.25% and 43%, respectively. S3 presented the most IoT-SCADA system architecture CSFs. The lowest-ranked studies did not adequately present the IoT-SCADA features. Therefore, S3 architecture provides the most appropriate reference architecture for an IoT-SCADA system architecture. Figure 3 depicts the proposed IoT-SCADA system architecture for the power utility company based on the MCDM matrix results in Table 4.

### The features of the proposed IoT-SCADA system

The proposed IoT-SCADA system architecture uses the highest-ranked studies categories of the MCDM matrix for the optimum design. The basis for the main components of the proposed architecture is from most of the selected relevant studies, except the S4, which used control centre servers as a substitute for the cloud. The main components of the IoT-SCADA system from S2 and S3 include smart sensors, RTU or data aggregator, IoT gateway, and the cloud.

Several studies outline the internet, fog computing, big data analytics, and IPv6 as the enabling technologies required for

**TABLE 3:** The Internet-of-Things-Supervisory Control and Data Acquisition system critical success factors.

| Study no | Article references | Smart sensors | Communication networks | Communication protocols | Internet | Fog computing | Cloud computing | Big data analytics |
|---|---|---|---|---|---|---|---|---|
| **IoT Critical Success Factors (CSFs)** | | | | | | | | |
| S1 | da Silva et al. (2016) | √ | X | √ | √ | X | √ | √ |
| S2 | Shahzad et al. (2017) | √ | √ | √ | √ | X | √ | √ |
| S3 | Yadav & Paul (2021) | √ | √ | √ | √ | √ | √ | X |
| S4 | Khan et al. (2017) | √ | √ | X | √ | X | X | X |
| S5 | Terruggia & Garrone (2020) | √ | X | √ | √ | √ | √ | √ |
| S6 | Nguyen-Hoang & Vo-Tan (2019) | X | X | √ | √ | X | √ | X |
| S7 | Tom & Sankaranarayanan (2017) | √ | √ | √ | √ | √ | √ | X |
| S8 | Shahzad & O'Nils (2018) | √ | √ | √ | √ | √ | √ | √ |
| S9 | Flaus (2019) | X | √ | √ | √ | √ | √ | X |
| S10 | Paul & Saraswathi (2017) | √ | √ | √ | √ | √ | √ | √ |

√, Available factors; X, Unavailable factors.

**TABLE 4:** Multi-Criteria Decision-Making matrix scoring results.

| Item no | Categories | Criteria | Weightings | Study (S) no | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | S1 | S2 | S3 | S4 | S5 | S6 | S7 | S8 | S9 | S10 |
| **Matrix-scoring table** | | | | **IoT-SCADA system architecture studies** | | | | | | | | | |
| **1** | **Main architecture components** | | **40.00%** | **25.00%** | **32.50%** | **36.25%** | **25.00%** | **25.00%** | **25.00%** | **25.00%** | **25.00%** | **25.00%** | **20.00%** |
| | | Smart sensors | 10.00% | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| | | RTU | 5.00% | 0.00 | 0.50 | 0.75 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| | | Gateway | 5.00% | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.00 |
| | | Cloud computing | 10.00% | 1.00 | 1.00 | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| | | Control center | 10.00% | 0.00 | 1.00 | 0.75 | 1.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **2** | **Enabling technologies** | | **20.00%** | **15.00%** | **10.00%** | **17.50%** | **1.25%** | **15.00%** | **5.00%** | **15.00%** | **11.25%** | **10.00%** | **20.00%** |
| | | Big data analytics | 5.00% | 1.00 | 1.00 | 0.75 | 0.25 | 1.00 | 0.00 | 0.00 | 0.50 | 0.00 | 1.00 |
| | | IPV6 | 5.00% | 1.00 | 0.00 | 0.75 | 0.00 | 0.00 | 0.00 | 1.00 | 0.00 | 1.00 | 1.00 |
| | | Internet | 5.00% | 1.00 | 1.00 | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| | | Fog computing | 5.00% | 0.00 | 0.00 | 1.00 | 0.00 | 1.00 | 0.00 | 1.00 | 0.75 | 0.00 | 1.00 |
| **3** | **Communication networks** | | **20.00%** | **6.25%** | **7.50%** | **11.25%** | **15.00%** | **3.75%** | **2.50%** | **11.25%** | **15.00%** | **15.00%** | **12.50%** |
| | | Wireless short-range communications | 5.00% | 0.50 | 0.00 | 0.75 | 1.00 | 0.25 | 0.25 | 0.50 | 1.00 | 1.00 | 1.00 |
| | | Wireless long-range communications | 5.00% | 0.75 | 1.00 | 0.75 | 1.00 | 0.50 | 0.25 | 0.75 | 1.00 | 1.00 | 1.00 |
| | | Cellular networks | 5.00% | 0.00 | 0.50 | 0.75 | 0.00 | 0.00 | 0.00 | 1.00 | 1.00 | 1.00 | 0.50 |
| | | Radio communication technologies | 5.00% | 0.00 | 0.00 | 0.00 | 1.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **4** | **Communication protocols** | | **20.00%** | **12.00%** | **1.00%** | **14.00%** | **2.00%** | **7.00%** | **10.50%** | **6.00%** | **3.50%** | **19.00%** | **6.00%** |
| | | 6LoWPAN | 6.00% | 1.00 | 0.00 | 0.75 | 0.00 | 0.00 | 0.00 | 1.00 | 0.50 | 1.00 | 1.00 |
| | | MQTT | 6.00% | 1.00 | 0.00 | 0.75 | 0.00 | 1.00 | 1.00 | 0.00 | 0.00 | 1.00 | 0.00 |
| | | CoAP | 6.00% | 0.00 | 0.00 | 0.75 | 0.00 | 0.00 | 0.50 | 0.00 | 0.00 | 1.00 | 0.00 |
| | | Other protocols | 2.00% | 0.00 | 0.50 | 0.25 | 1.00 | 0.50 | 0.75 | 0.00 | 0.25 | 0.50 | 0.00 |
| **5** | **Total score** | | 100.00% | 58.25% | 51.00% | 79.00% | 43.25% | 50.75% | 43.00% | 57.25% | 54.75% | 69.00% | 58.50% |

optimum system operation of the IoT-SCADA system. However, S6 did not effectively apply the enabling technologies. Technology such as fog computing is essential for pre-processing data and thus reduces latency and data bottlenecks for the cloud (Terruggia & Garrone 2020). Furthermore, the IPv6 enables the identification of a vast number of devices. At the same time, big data analytics ensures seamless analysis of the enormous data from the IoT devices for the business and technical decision-making process (Paul & Saraswathi 2017).

On communication networks, wireless short-range and long-range communication technologies and cellular networks are recommended for communication between devices. S4, S8, and S9 adequately presented the mentioned communication networks. The proposed architecture uses Wi-Fi for communication between the smart sensors and the gateway and long-range communication technologies between the smart sensor and the cloud. The recommended long-range technologies include GPRS/GPS, 4G, and 5G for communication between the cloud, gateway, control centre, and SCADA engineering workstation (Khan et al. 2017; Shahzad & O'Nils 2018). The optical fibre is a backup link for communication between devices.

The recommended IoT protocols for the proposed architecture include the MQTT and Constrained Application Protocol (CoAP) protocols used for communication between smart sensors or IoT gateway and the cloud (Nguyen-Hoang & Vo-Tan 2019), and the IPv6 over Low power Wireless Personal Area Network (6LowPAN) protocol for communication between the gateway and smart sensors (Da Silva et al. 2016). Study S1, S3, and S9 support the selected protocols.

### Enterprise systems integration and the proposed IoT-SCADA system architecture

The recommended IoT-SCADA system architecture indicates the interconnection of various enterprise systems (see Figure 3). Level 0 – 4 of the architecture depicts the reference model to the ISA 99 standard and the Purdue model for a control hierarchy. The architecture shows the logical framework of device operating levels, hierarchy, and the main activity at each level. The levels further indicate the environment of various system devices, with level 0 and 1 devices representing systems in the field, including substation building.

The proposed architecture uses firewalls for network segmentation and to protect enterprise systems against cyber-attacks. The proposed architecture's networking layer and cloud computing ensure continuous data flow between the ICS and ERP, thus enabling remote control and monitoring. Additionally, the proposed architecture systems have three segments that demonstrate the three layers of the IoT system architecture.

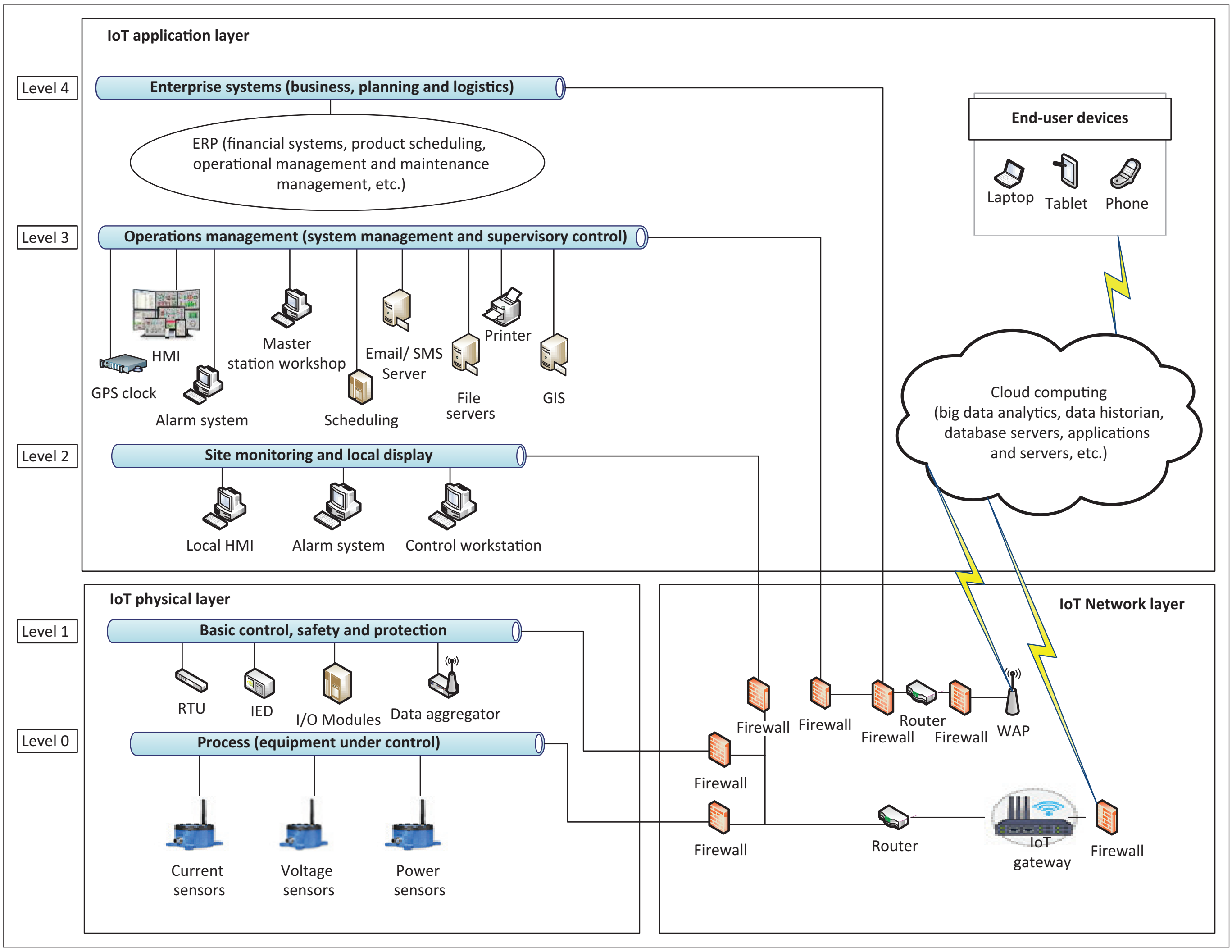

IoT application layer
Level 4
Enterprise systems (business, planning and logistics)
ERP (financial systems, product scheduling, operational management and maintenance management, etc.)
Level 3
Operations management (system management and supervisory control)
HMI
GPS clock
Alarm system
Master station workshop
Email/ SMS Server
Scheduling
Printer
File servers
GIS
Level 2
Site monitoring and local display
Local HMI
Alarm system
Control workstation
End-user devices
Laptop
Tablet
Phone
Cloud computing (big data analytics, data historian, database servers, applications and servers, etc.)
IoT physical layer
Level 1
Basic control, safety and protection
RTU
IED
I/O Modules
Data aggregator
Level 0
Process (equipment under control)
Current sensors
Voltage sensors
Power sensors
IoT Network layer
Firewall
Firewall
Router
Firewall
Firewall
WAP
Firewall
Firewall
Router
IoT gateway
Firewall

**FIGURE 3:** The proposed Internet-of-Things-Supervisory Control and Data Acquisition system architecture (author's design).

The IoT layers depicted in Figure 3 only show how IoT alters the third generation SCADA system integration and operation of the power utility company and do not indicate any geographical properties of the system components. The proposed architecture combines networked SCADA with IoT to form the IoT-SCADA system.

## Proposed IoT-SCADA versus existing power utility company SCADA system

The data collection concerning the existing utility company SCADA system is through the power utility company verification. The existing power utility company SCADA generation is the networked SCADA systems, that is, the third generation. The proposed IoT-SCADA system from this study is the fourth-generation SCADA system.

The comparison of the two distinct SCADA generations is as follows:

- Main architecture components: The proposed IoT-SCADA system architecture's main components include intelligent sensors, RTUs, IoT gateways and cloud computing, and the communication between all elements is wireless (Da Silva et al. 2016; Nguyen-Hoang & Vo-Tan 2019; Terruggia & Garrone 2020). The access to the HMI, control centre, data historian server and other applications is through the cloud.
- In comparison, the networked SCADA consists of sensors, IEDs, RTUs, MTU, HMI, data historian servers and front-end servers as separate systems per utility company architecture.
- Enabling technologies: The proposed IoT-SCADA system supporting technologies include IPv6, big data analytics, internet, and fog and cloud computing (Paul & Saraswathi 2017; Yadav & Paul 2021). In contrast, the utility company's networked SCADA system enabling technologies include the LAN and WAN for sending data to a central-control station SCADA server, in contrast to the IoT-SCADA system cloud computing component.
- Communication networks: The power utility company networked SCADA system uses a combination of various communication networks, such as GPRS, GSM, radio, optical fibre, Ethernet, copper, and a mixture of the indicated communication mediums. In contrast, the IoT-SCADA system uses short-range and long-range wireless communication technologies such as GPRS, Wi-Fi,

Bluetooth and mobile networks (e.g. 5G) (Khan et al. 2017; Tom & Sankaranarayanan 2017).

- Communication protocols: The IoT-SCADA system uses IP-based protocols such as MQTT, CoAP, 6LoWPAN and TCP/IP (Flaus 2019; Yadav & Paul 2021). In contrast, the networked SCADA uses serial and ethernet communication-based protocols such as DNP3, Modbus, IEC 61850 and IEC 60870-5-101/104.
- System security: The power utility company's IT department is responsible for protecting the networked SCADA system. The protection measures include the security firewalls between the SCADA system and IT network, login authentication and authorisations on devices, and physical security throughout the SCADA system network. Other security measures depend on the service level agreement (SLA) with the service providers. In the proposed IoT-SCADA system, the cloud service companies are responsible for data and the servers' security. Therefore, the security also depends on the SLA with the cloud service providers. Furthermore, the service providers are responsible for the maintenance and improvements of the system (Flaus 2019; Yadav & Paul 2021). The security measures for the IoT-SCADA system include cryptography mechanisms such as the Advanced Encryption Standard (AES) algorithm to secure the system against authentication and privacy threats (Da Silva et al. 2016; Holakar et al. 2016; Shahzad et al. 2017). To protect the business and users against cyber threats, the interface to the company with the cloud in the proposed architecture is through firewalls. Furthermore, the support of authentication by the IoT protocols such as MQTT provides extra data security (Mohamad Noor & Hassan 2019).
- Advantages of the architectures: In the networked SCADA system, there is less dependence on the third parties and fewer devices in the network, thus resulting in more privacy and fewer security threat points, that is, a reduced attack surface. Nevertheless, the IoT-SCADA system provides more flexibility, scalability, less cabling, interoperability, and lower implementation costs (Rani et al. 2015). Other benefits depend on selecting the appropriate components, such as the cloud deployment model and the SLAs with the cloud service providers in the proposed IoT SCADA system.

**Impact of the proposed Internet-of-Things-Supervisory Control and Data Acquisition system on the power utility company:** The impact of the proposed IoT-SCADA system architecture on the power utility company operations is as follows:

- Improved network visibility – The proposed architecture can ensure that the utility company achieves 100% network visibility because of the wireless communication infrastructure (Dual 5G service providers are used) and data availability for business and technical insights.
- Reliable communication – Most often, theft and vandalism affect the current power utility company's SCADA system communication infrastructure. However, the IoT-SCADA wireless communication for both short-distance and long-distance ensures reliable communications and improves the availability of power networks to power system operators.
- Quick project delivery – Wireless communication devices of the IoT-SCADA system can ensure a faster turnaround time because of reduced system integration effort and costs.
- Network security – The use of firewalls and other cyber-attack countermeasures between various business levels and systems provides trusted and secure zones and conduits for data flow in the organisation.
- Information accessibility – The use of cloud computing ensures that authorised and authenticated personnel through multi-factor authentication (MFA) can access information anytime and anywhere, thus improving service delivery.

**The benefits of the proposed IoT-SCADA system architecture:** The benefits of the proposed SCADA architecture are as follows (Babayigit & Sattuf 2019; Pramudhita et al. 2018; Terruggia & Garrone 2020):

- Scalability – The system can accommodate an enormous number of devices.
- Interoperability – Enable seamless integration of various heterogeneous devices to interact and share data through the internet/cloud.
- Flexibility – The IoT-SCADA system is expandable and allows for easy removal or addition of devices.
- Big data analytics – To prevent equipment failures and ensure ease of maintenance, the big data analytics function enables analysis of data from field devices for predictive and prescriptive maintenance of assets, thus improving asset maintenance and reducing maintenance costs (e.g. overtime) because of a reliable power network.

## Research conclusion, limitations, and future work

### Conclusion

This study discussed many facets of SCADA systems and enterprise systems integration, focusing on power utility SCADA systems through literature and a case study.

The first research question is answered by steps 1–6, see Figure 2. Firstly, relevant IoT-SCADA systems literature is identified through academic database search, and CSFs are obtained through literature review. The identified CSFs for the IoT-SCADA system are as follows:

- The main standard system components include intelligent sensors, IoT gateways and cloud computing.
- The supporting features include fog computing, IPv6, internet and big data analytics.
- Wireless short-range and long-range communications and cellular networks are appropriate for communications between devices or components of the system.
- Seamless communication between devices enabled by protocols such as MQTT, CoAP and the IPv6 over 6LowPAN is applicable.

Furthermore, the research compared 10 IoT-SCADA system architectures using the MCDM matrix of identified CSFs to propose an IoT-SCADA system architecture for optimum integration of the power utility company SCADA system.

The second research question is answered by comparing the existing power utility company SCADA system with the proposed IoT-SCADA system architecture based on the CSFs for an IoT-SCADA system architecture. The research further concludes that the IoT-SCADA system has potential to resolve most of the challenges found in the legacy SCADA system generations. In the case study, the problems are associated wih the third generation SCADA system.

The third research question is answered by presenting the impact and benefits of the proposed IoT-SCADA system compared with the power utility company.

Finally, the researchers found that the proposed IoT-SCADA system architecture has the potential to resolve many of the challenges encountered in previous generations of SCADA system architectures. For example, the cloud provides a platform for shared analytics services, which in the previous generation software packages had to be installed on local machines.

### Limitations

The data collection process did not include consultation of the SCADA system specialists concerning the IoT-SCADA system CSFs identification and matrix categories weightings.

### Future work

Future research should consider a pilot project to demonstrate the actual IoT-SCADA system integration and operation to prove the implementation practicality.

## Acknowledgements

The authors thank U.J. for research support.

### Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

### Authors' contributions

S.S.P. conducted this research to accomplish an MPhil degree in Engineering Management at the University of Johannesburg under the supervision of A.T. and M.C.S.

### Ethical considerations

This study followed all ethical standards for research without direct and indirect contact with human or animal subjects.

### Funding information

This research work received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

### Data availability

Data that support the findings of this research are available upon request from the main or corresponding author, S.S.P.

### Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

## References

Ackerman, P., 2017, 'Industrial cybersecurity -1.3 The Purdue Model for industrial control systems', in S. Srivastava, V. Boricha, H. Bhavsar, S. Dias & V.K. Mewada (eds.), *Industrial cybersecurity*, pp. 6–31, Packt Publishing, Birminham.

Aly, M., Khomh, F. & Yacout, S., 2021, 'What do practitioners discuss about IoT and industry 4.0 related technologies? Characterisation and identification of IoT and industry 4.0 categories in stack overflow discussions', *Internet of Things* 14, 100364. https://doi.org/10.1016/j.iot.2021.100364

April, A., Ouanouki, R. & Morales, G.A., 2014, *Should the cloud computing definition include a big data perspective?*, pp. 1–6, IGI Global, Montreal.

Babayigit, B. & Sattuf, H., 2019, *An IIoT and web-based low-cost SCADA system for industrial automation*, pp. 890–894, IEEE, Bursa.

Bobat, A., Gezgin, T. & Aslan, H., 2015, 'The SCADA system applications in management of yuvacik dam and reservoir', *Desalination and Water Treatment* 54(8), 2108–2119. https://doi.org/10.1080/19443994.2014.933615

Borgaonkar, R. & Jaatun, M.G., 2019, *5G as an enabler for secure IoT in the smart grid: Invited paper*, pp. 1–7, IEEE, Krakow.

Binder, C., Brankovic, B., Neureiter, C. & Lüder, A., 2020, *Lessons learned from developing industrial applications according to RAMI 4.0 by applying model based systems engineering*, pp. 883–888, IEEE, Vienna.

Da Silva, A.F., Ohta, R.L., Dos Santos, M.N. & Binotto, A.P.D., 2016, 'A cloud-based architecture for the internet of things targeting industrial devices remote monitoring and control', *International Federation of Automation Control (IFAC) Papers Online* 49(30), 108–113. https://doi.org/10.1016/j.ifacol.2016.11.137

De Melo, P.F.S. & Godoy, E.P., 2019, *Controller interface for industry 4.0 based on RAMI 4.0 and OPC UA*, pp. 229–234, IEEE, Naples.

Dolezilek, D., Gammel, D. & Fernandes, W., 2019, *Complete IEC 61850 protection and control system cybersecurity is so much more than device features based on IEC 62351 and IEC 62443*, pp. 1–9, Schweitzer Engineering Laboratories, IEEE, Pullman, WA.

Filkins, B. & Doug, W., 2018, *SANS institute information security reading room – The 2018 SANS industrial IoT security survey: Shaping IIoT security concerns*, pp. 1–21, SANS Institute Company, Scandanavia, viewed 30 March 2021, from https://forescout-wpengine.netdna-ssl.com/wp-content/uploads/2018/07/2018-SANS-Industrial-IoT-Security-Survey.pdf.

Flaus, J., 2019, 'Architecture and communication in an industrial control system', in *Cybersecurity of industrial systems*, pp. 25–55, John Wiley & Sons, Hoboken, NJ.

Hain, M., Moutachaouik, H., Zakrani, A. & Enaanai, A., 2017, 'A new approach to MES system deployment', *International Journal of Scientific Engineering and Technology* 6(6), 198–202. https://doi.org/10.5958/2277-1581.2017.00019.5

Holakar, A., Mahendra, L., Prasad, G.L.G. & Shetter, R., 2016, *Secure interoperable gateway for wireless SCADA system*, pp. 125–129, Computer Science, Bangalore.

Hong, C., Xia, L. & Guangrong, L., 2020, *Application of fuzzy-set qualitative comparative analysis on enterprise asset allocation, organizational ambidexterity and innovation performance*, pp. 11–16, IEEE, Zhengzhou.

Hossain, M.S., Rahman, M., Sarker, M.T., Haque, M.E. & Jahid, A., 2019, 'A smart IoT-based system for monitoring and controlling the sub-station equipment', *Internet of Things* 7, 100085. https://doi.org/10.1016/j.iot.2019.100085

ISA 99, 2007, *Security for industrial automation and control systems part 1: Terminology, concepts, and models: ANSI/ISA 99*, pp. 1–95, viewed 28 March 2021, from https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

Ivanković, I., Peharda, D., Novosel, D., Ẑubrinic-Kostović, K. & Kekelj, A., 2018, *Smart grid substation equipment maintenance management functionality based on control center SCADA data Ksenija Zubrinic-Kostovic HOPS*, pp. 1–10, CIGRE, Paris.

Januário, F., Carvalho, C., Cardoso, A., & Gil, P., 2016, *Security challenges in SCADA systems over wireless sensor and actuator networks*, pp. 363–368, IEEE, Lisbon.

Kaur, K., 2018, *A survey on internet of things – Architecture, applications, and future trends*, pp. 581–583, IEEE, Jalandhar.

Khan, W.Z., Aalsalem, M.Y., Khan, M.K., Hossain, Md.S. & Atiquzzaman, M., 2017, *A reliable internet of things based architecture for oil and gas industry*, pp. 705–710, IEEE, PyeongChang.

Kumar, A., Sah, B., Singh, A.R., Deng, Y., He, X., Kumar, P., Hangzhou, P.R.China., 2020, *Decision making applications in modern power systems*, pp. 1–40, Academic Press, MA.

Li, S., Jiang, B., Wang, X. & Dong, L., 2017, 'Research and application of a SCADA system for a microgrid', *Technologies (Basel)* 5(2), 1–11. https://doi.org/10.20944/preprints201703.0068.v2

Lundius, A., 2019, *Initial assessment of manufacturing execution systems*, Royal Institute of Technology, Stockholm, pp. 3–17, viewed 20 February 2021, from https://kth.diva-portal.org/smash/get/diva2:1374272/FULLTEXT01.pdf.

Madala, S., Herink, A., Robinette, M., Ramaekers, T., Palk, R. & Brewer, D., 2018, *Improvements in rural load management by electric cooperatives through an effective SCADA system, and distribution connected generation*, pp. 106–113, IEEE, Memphis, TN.

Mohamad Noor, M.B. & Hassan, W.H., 2019, 'Current research on internet of things (IoT) security: A survey', *Computer Networks* 148, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

Nguyen-Hoang, P. & Vo-Tan, P., 2019, *Development an open-source industrial IoT gateway,* Institute of Electrical and Electronics Engineering, pp. 201–204, Ho Chi Minh City.

Nigel, S. & Vera, S., 2017, *Qualitative comparative analysis (QCA)*, pp. 1–5, INTRAC for Civil Society, INTRAC.org, viewed 22 April 2021, from https://www.intrac.org/wpcms/wp-content/uploads/2017/01/Qualitative-comparative-analysis.pdf.

Obregon, L. & Barbara, F., 2015, *SANS institute information security reading room – Secure architecture for industrial control systems*, pp. 1–26, SANS Institute, Scandanavia.

Pappas, I.O., Kourouthanassis, P.E., Giannakos, M.N. & Chrissikopoulos, V., 2016, 'Explaining online shopping behavior with fsQCA: The role of cognitive and affective perceptions', *Journal of Business Research* 69(2), 794–803. https://doi.org/10.1016/j.jbusres.2015.07.010

Patel, K.K., Patel, S.M. & Scholar, P.G., 2016, *Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges*, pp. 6122–6131, International Journal of Engineering Science and Computer, Vadodara.

Paul, P.V. & Saraswathi, R., 2017, *The internet of things – A comprehensive survey*, pp. 421–426, IEEE, Melmaruvathur.

Postolache, O.A., Sazonov, E. & Mukhopadhyay, S.C., 2019, 'Chapter 6: IoT-enabled water monitoring and control for smart city', in *Sensors in the age of the internet of things – Technologies and applications*, pp. 140–169, Institution of Engineering and Technology, Lucknow.

Pramudhita, A.N., Asmara, R.A., Siradjuddin, I. & Rohadi, E., 2018, 'Internet of Things integration in smart grid', in *2018 International Conference on Applied Science and Technology (iCAST)*, Malang, Indonesia, October 26–27, 2018, pp. 718–722.

Rajeswar, M.K., 2019, *Industry 4.0 wave -relevance of SCADA in an IOT world and journey towards a true digital enterprise*, pp. 78–88, Institute of Electrical and Electronics Engineers (IEEE), viewed 30 March 2021, from http://site.ieee.org/indiacouncil/files/2019/10/p78-p88.pdf.

Rani, B.K., Rani, B.P. & Babu, A.V., 2015, 'Cloud computing and inter-clouds – Types, topologies and research issues', *Procedia Computer Science* 50, 24–29. https://doi.org/10.1016/j.procs.2015.04.006

Shahzad, A., Kim, Y. & Elgamoudi, A., 2017, *Secure IoT platform for industrial control systems*, pp. 1–6, IEEE, Busan.

Shahzad, K. & O'Nils, M., 2018, *Condition monitoring in industry 4.0 – Design challenges and possibilities: A case study*, pp. 101–106, Institute of Electrical and Electronics Engineering, Brescia.

Sighania, M. & Kinker, R., 2015, 'Tata power delhi distribution: Automation vs manpower', *Vikalpa* 40(1), 97–113. https://doi.org/10.1177/0256090915573611

Stanimirović, A., Bogdanović, M., Frtunić, M. & Stoimenov, L., 2020, 'Low-voltage electricity network monitoring system: Design and production experience', *International Journal of Distributed Sensor Networks* 16(1), 1550147720903629.

Subramanian, C., 2017, *Global conference and exhibition on 'innovative solutions in flow measurement & control. Oil, water & gas'*, pp. 1–7, Aryanet Institute of Technology, Velikkad.

Tejas Kopte, A.P., 2015, 'A study on power system automation', *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 4(9), 7605–7610. https://doi.org/10.15662/IJAREEIE.2015.0409030

Terruggia, R. & Garrone, F., 2020, *Secure IoT and cloud based infrastructure for the monitoring of power consumption and asset control*, pp. 1–6, IEEE, Catania.

Tom, R.J. & Sankaranarayanan, S., 2017, *IoT based SCADA integrated with fog for power distribution automation*, pp. 1–4, IEEE, Lisbon.

Upadhyay, D. & Sampalli, S., 2020, 'SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations', *Computers & Security* 89, 101666. https://doi.org/10.1016/j.cose.2019.101666

US ICS-CERT, 2016, *Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies industrial control systems cyber emergency response team*, pp. 1–49, US Department of Homeland Security, viewed 30 March 2021, from https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

Wang, Y., Towara, T. & Anderl, R., 2017, *Topological approach for mapping technologies in reference architecture model industry 4.0 (RAMI 4.0)*, pp. 1–9, World Congress Engineering Computer Science, San Francisco, CA.

Yadav, G. & Paul, K., 2021, 'Architecture and security of SCADA systems: A review', *International Journal of Critical Infrastructure Protection* 34, 100433. https://doi.org/10.1016/J.IJCIP.2021.100433

Zawra, L.M., Mansour, H.A. & Messiha, N.W., 2019, *Migration of legacy industrial automation systems in the context of industry 4.0 – A comparative study*, pp. 1–7, IEEE, Manama.